サイバー戦争の「謎」を探る――サイバー安全保障有識者会議と政府の思惑

JCA-NET セミナー

2024 年 7 月 27 日

小倉利丸

toshi@jca.apc.org

サイバー戦争の「謎」を探る——サイバー安全保障有識者会議と政府の思惑

6 月 7 日にサイバー安全保障分野での対応能力の向上に向けた有識者会議が開催されました。この会議がこの間争点になってきた能動的サイバー防御の法制化を検討する中心的な存在になります。この第一回会議で、官民の情報共有・民間支援、通信情報の利用、攻撃者のサーバ等の無害化を中心的な検討課題とすることが決まり、これらについて個別に会合を設定することも決定されました。有識者会議には内閣官房サイバー安全保障体制整備準備室が「サイバー安全保障分野での対応能力の向上に向けて」と題する資料を提出しました。この資料が今後の有識者会議の方向に大きく影響するものと思われます。

この内閣官房の資料には、たとえば、 Wannacry 、 Volt Typhoon 、 Black Tech 、 Living-off-the-Land 、 pre-positioning など馴染のない言葉が頻発します。そのために、能動的サイバー防御として政府が何を狙いとしているのか、その意図すら曖昧にされています。実は、こうした耳慣れない言葉のなかに、政権が意図するサイバー領域における先制攻撃の重要なヒントも隠されています。

セミナーでは、この内閣官房の資料を取り上げます。特に Volt Typhoon や pre-positioning など深刻な先制攻撃の危険性とも関連しうる問題について議論してみたいと思います。

基本的な観点

(1) 戦争放棄

不戦条約(1928)

第１条　締約国は、国際紛争解決のために戦争に訴えることを非難し、かつ、その相互の関係において国家政策の手段として戦争を放棄することを、その各々の人民の名において厳粛に宣言する。

第２条　締約国は、相互間に発生する紛争又は衝突の処理又は解決を、その性質または原因の如何を問わず、平和的手段以外で求めないことを約束する。

憲法９条

日本国民は、正義と秩序を基調とする国際平和を誠実に希求し、国権の発動たる戦争と、武力による威嚇又は武力の行使は、国際紛争を解決する手段としては、永久にこれを放棄する。②　前項の目的を達するため、陸海空軍その他の戦力は、これを保持しない。国の交戦権は、これを認めない。

基本的な観点

(2) 通信の秘密、表現、思想信条の自由

世界人権宣言

12条 何人も、自己の私事、家族、家庭若しくは通信に対して、ほしいままに干渉され、又は名誉及び信用に対して攻撃を受けることはない。

19条 すべて人は、意見及び表現の自由に対する権利を有する。この権利は、干渉を受けることなく自己の意見をもつ自由並びにあらゆる手段により、また、国境を越えると否とにかかわりなく、情報及び思想を求め、受け、及び伝える自由を含む。

憲法21条

集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。

② 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

基本的な観点

上記の条約や憲法はインターネットの出現前に制定されているが、時代を超えた普遍的な観点である。

しかし、インターネットが国家インフラとして重要な役割を果している現在、戦争放棄と表現の自由、通信の秘密の権利を確保するためには、従来の戦争や人権の枠組を見直す必要がある。

政府のスタンスは

- 日本はサイバー攻撃の被害者である
- 通信の秘密よりも公共の福祉が優先する

しかし、この前提を受け入れるべきではない。

- 日本はサイバー攻撃の加害者である
- 通信の秘密に公共の福祉の制約を課すべきではない

サイバー安全保障有識者会議

「国家安全保障戦略」（2022 年 12 月 16 日閣議決定）に基づき、「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるべく、当該分 野における新たな取組の実現のために必要となる法制度の整備等について検討を行う」

https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html

- 6 月 7 日第一回会合
- 三つの部会を設置
  - 官民の情報共有・民間支援
  - 通信情報の利用
  - 攻撃者のサーバ等の無害化
- 7 月 8 日第二回会合

サイバー安全保障有識者会議

第一回（政府側） 岸田 文雄 内閣総理大臣 河野 太郎 国務大臣 村井 英樹 内閣官房副長官 石川 昭政 副大臣 栗生 俊一 内閣官房副長官 2 秋葉 剛男 国家安全保障局長 藤井 健志 内閣官房副長官補 市川 恵一 内閣官房副長官補 鈴木 敦夫 内閣官房副長官補 飯田 陽一 内閣審議官

第二回（政府側） 河野 太郎 国務大臣 石川 昭政 副大臣 秋葉 剛男 国家安全保障局長 阪田 渉 内閣官房副長官補 市川 恵一 内閣官房副長官補 2 鈴木 敦夫 内閣官房副長官補 飯田 陽一 内閣審議官 小柳 誠二 内閣官房サイバー安全保障体制整備準備室長 木村 公彦 内閣官房サイバー安全保障体制整備準備室長代理（元総務） 佐野 朋毅 内閣官房サイバー安全保障体制整備準備室次長 中溝 和孝 内閣官房サイバー安全保障体制整備準備室次長 門松 貴 内閣官房サイバー安全保障体制整備準備室次長 飯島 秀俊 内閣官房サイバー安全保障体制整備準備室次長 室田 幸靖 内閣審議官 関口 祐司 内閣審議官

【連絡先】

内閣官房サイバー安全保障体制整備準備室

〒100-0014　東京都千代田区永田町 2-4-12

TEL.03-6205-4169

サイバー安全保障分野での対応能力の向上に向けた有識者会議　構成員

（五十音順）

氏名	所属
上沼　紫野	LM 虎ノ門南法律事務所弁護士
遠藤　信博	日本電気株式会社特別顧問
落合　陽一	筑波大学デジタルネイチャー開発研究センター長/准教授
川口　貴久	東京海上ディーアール株式会社主席研究員
川添　雄彦	日本電信電話株式会社代表取締役副社長 副社長執行役員 一般社団法人 電気通信事業者協会参与 一般社団法人 ICT-ISAC 理事
酒井　啓亘	早稲田大学法学学術院教授
佐々江　賢一郎	公益財団法人 日本国際問題研究所理事長
宍戸　常寿	東京大学大学院法学政治学研究科教授
篠田　佳奈	株式会社 BLUE 代表取締役
辻　伸弘	SB テクノロジー株式会社プリンシパルセキュリティリサーチャー
土屋　大洋	慶應義塾大学大学院政策・メディア研究科教授
野口　貴公美	一橋大学副学長、法学研究科教授
丸谷　浩史	株式会社日本経済新聞社常務執行役員 大阪本社代表
村井　純	慶應義塾大学教授
山岡　裕明	八雲法律事務所弁護士
山口　寿一	株式会社読売新聞グループ本社代表取締役社長
吉岡　克成	横浜国立大学大学院環境情報研究院/先端科学高等研究院教授

有識者会議の議論の見方

- 原則(戦争放棄、人権)の観点から判断する
- 被害感情や国際情勢への不安感情を煽る言動にまどわされない
- 既存の自衛隊や警察の制度を既成事実として前提する議論に与しない
- サイバー領域は武器・兵器による殺傷行為と直接関係ないと思いこんではいけない
- 専門的にみえる議論の「わかりにくさ」は、反対の世論を抑える政府の作戦である
- 議員も有権者も素人。民主主義では素人が立法の主体。専門家に判断を委ねてはいけない

サイバー戦争の具体例
ガザ戦争の場合

戦争前から保有する
ガザ住民に関する
個人情報

リアルタイム
での動静把握
(ドローンなど)

ターゲットの
選択
ハマースの幹部
ハマースの下級兵士
医療関係
ジャーナリスト
国際援助団体
一般市民
(ラベンダー、福音)

Google 、 Amazon
などの
解析技術支援
(Project Nimbus)

ターゲットへの
攻撃
巻き添え
の犠牲も折り込み済み

軍の実行部隊
への指示

国際ジャーナリスト
などの退去
ジェノサイドの実態
把握をさせない

イスラエル国内
の SNS による
プロパガンダ

ヘイトスピーチ
偽情報の拡散

反戦運動への監視

SNS などでの
情報操作、検閲

X 、 Facebook
など SNS 企業の
技術支援

ガザの
通信遮断

最近のサイバー攻撃の動向
(Volt Typhoon)

最近のサイバー攻撃の動向（事前配置(pre-positioning)活動）

2023年５月、ファイブ・アイズ５か国及びマイクロソフト社が、中国背景とされるサイバー攻撃グループVolt Typhoonについて、注意喚起を発出。概要以下のとおり。

- 有事における機能不全を念頭に置いた、**重要インフラへの事前のアクセス確保**（pre-positioning）を目的としたサイバー攻撃が発生

- 長期間の潜伏に必要な**高度な検知回避能力**が特徴
  - ✓ ネットワーク機器の脆弱性を突いて侵入。ゼロデイ脆弱性も悪用
  - ✓ マルウェアを使わず、正規ユーザになりすまし、正規ツールを駆使（Living off the Land）
  - ✓ 侵入痕跡となるログの消去 等

- 米国においては、本土及び島嶼部の米軍基地にサービスを提供する重要インフラ（通信、エネルギー、水道など）への攻撃の脅威が高まっている

（出典）PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (2024.2) 等

有識者会議第一回会議資料

最近のサイバー攻撃の動向
(Volt Typhoon)

Volt Typhoon とは

2023 年 5 月マイクロソフトが注意喚起

※ 民間企業が最初に注意喚起していることに注目

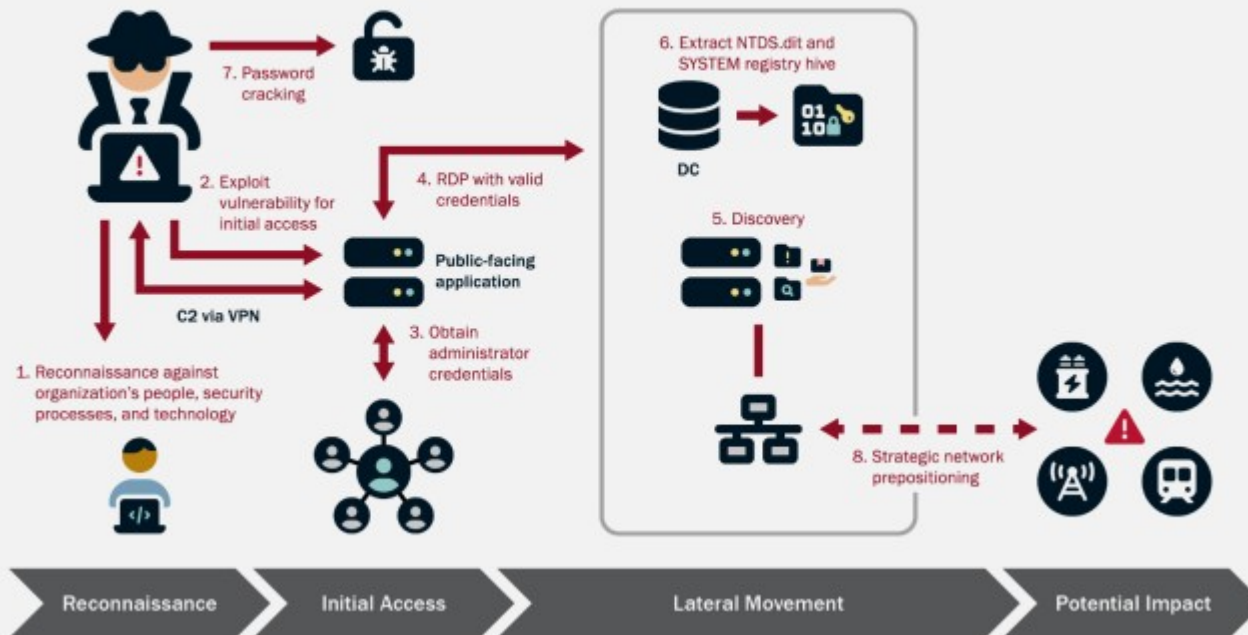
- 重要インフラへの事前のアクセス (pre-positioning) を確保
- 長期に潜伏し、発見されないように検知機能を回避する
  - ネットワークの脆弱性を利用する
  - 正規の利用者になりすます
  - 侵入の痕跡を消去する
- 米国本土とグアムで発生

最近のサイバー攻撃の動向
(Volt Typhoon)

事例として挙げられている Volt Typhoon は、長期にわたって標的のシステムに密かに潜伏して情報を収集する行動をとる。標的のなかには米軍基地のあるグアムも含まれていた。基地だけでなく、通信、製造、公益事業、交通、建設、海運、政府、情報技術、教育のインフラも狙われたという。 Volt Typhoon は、上のスライドでも指摘されているように、マイクロソフトがその存在を把握して公表したことで知られるようになった。米国の場合ですら、サイバー領域のリスクや脅威を軍や政府の情報機関が網羅的に把握できるわけではない。

Pre-positioning について。

- 長期にわたって標的とされるシステムなどに、事前に配置 (pre-positioning) されることをいう。
- こうした行動によって、地政学的軍事的緊張や衝突の際に重要インフラなどへの破壊行動をとれるようにする。
- 伝統的なサイバースパイ活動や軍事作戦とは一致せず、複数の重要インフラ部門にわたる OT 機能 (次ページ参照) の破壊を可能にするために、ネットワーク上に事前に配備される。

最近のサイバー攻撃の動向 (Volt Typhoon)

図版の出典はここ

1.組織の人間、セキュリティ、プロセス、テクノロジーについての予備調査 (Reconnaissance)

2.初期アクセスのための脆弱性の利用

3.管理者資格の取得

4.有効な資格を有する Remote Desktop Protocol

5.発見

6.NTDS.dit とシステム レジストリ ハイヴの取得

7.パスワードクラッキング

8.戦略的なネットワーク prepositioning

多くの事例は、自国を被害者と想定した事例になっているが、実際には、自国が攻撃者となる事例として「読む」必要がある。

能動的サイバー防御とは、ここで例示されているような行動をとることも含まれる、と解釈してよい。

最近のサイバー攻撃の動向
(Volt Typhoon)

(補足説明)OT 機能とは

製造業・社会インフラの「制御・運用技術の総称」

OT(Operational Technology) とは、工場や発電所などに使われる、物理的なシステムや設備を最適に動かすための制御・運用技術の総称です。具体的には、製品や部品の製造を行うロボットや、工場でのセンサーによる温度監視などの用途があります。

OT が使われるのは、基本的に工場や発電所などの閉じられた環境、つまり「クローズド」です。代表的なシステムとしては、外部機器を自動制御する「 PLC(Programmable Logic Controller) 」や工場やプラントで使われる分散制御システムの「 DCS(Distributed Control System) 」、管理制御およびデータ収集システムの「 SCADA(Supervisory Control and Data Acquisition) 」などが挙げられます。

https://www.ntt.com/business/services/rink/knowledge/archive_08.html

最近のサイバー攻撃の動向
(Volt Typhoon)

なぜ Volt Typhoon なのか？

内閣官房のスライドの説明がもっぱら中国のケースに集中しているところに違和感がある。今後日本の能動的サイバー防御のひとつの手段になりうるかもしれない。中国がやっているこの技術を米国など他の諸国が真似しないはずがない。同様の仕組みの開発が進むはずだ。しかも Volt Typhoon のような機能は日本のように「防衛」を前面に出して監視するシステムを好む場合にはかなり有効な手段とみなしているのではないか。軍だけでは完結できないので、民間や政府の他の非軍事機関との連携が必須になる。その結果として、社会のシステム全体が軍事安全保障にひきづられることになる。

能動的サイバー防御の重要な柱のひとつが、極めて侵襲性の大きい諜報活動になるのではないか、ということだ。

ただし、中国側は、 Volt Typhoon を営利目的の犯罪とみている。

中国のレポート
https://www.cverc.org.cn/head/zhaiyao/futetaifengEN.pdf

最近のサイバー攻撃の動向
(Volt Typhoon)

このVolt Typhoonをどのようにして撃退したのか

- 米司法省と連邦捜査局（ＦＢＩ）が同集団の活動を遠隔操作で無効化する法的許可を得る(ロイター2024年1月の報道)
- 作戦には数ヶ月を要した

NTT(NTT セキュリティ・ジャパン株式会社、コンサルティングサービス部 OSINT モニタリングチーム)『サイバーセキュリティレポート2024.02』

かなりのページを割いてVolt Typhoonに言及

日本語で読める最も詳しい記述のひとつ

こうしたレポートが防衛省や政府機関ではなく民間の通信事業者から公表されているということがサイバー安全保障の重要な特徴である。従来は軍需産業とはみなされてこなかった民間通信事業者へに対しても関心を向けることが必要になる。

最近のサイバー攻撃の動向
(Volt Typhoon)

Volt Typhoon から「能動的サイバー防御」に関して私たちが見過してはならない論点とは

- Volt Typhoon のような攻撃を日本が実行する可能性を念頭に置くことが必要
- 戦争状態の有無とは無関係に、長期にわたる相手のサイバー領域の状況を把握する作業がある。
  - 相手のシステムの脆弱性の探知
  - システムの全容把握
  - システム管理者などの人間関係の把握

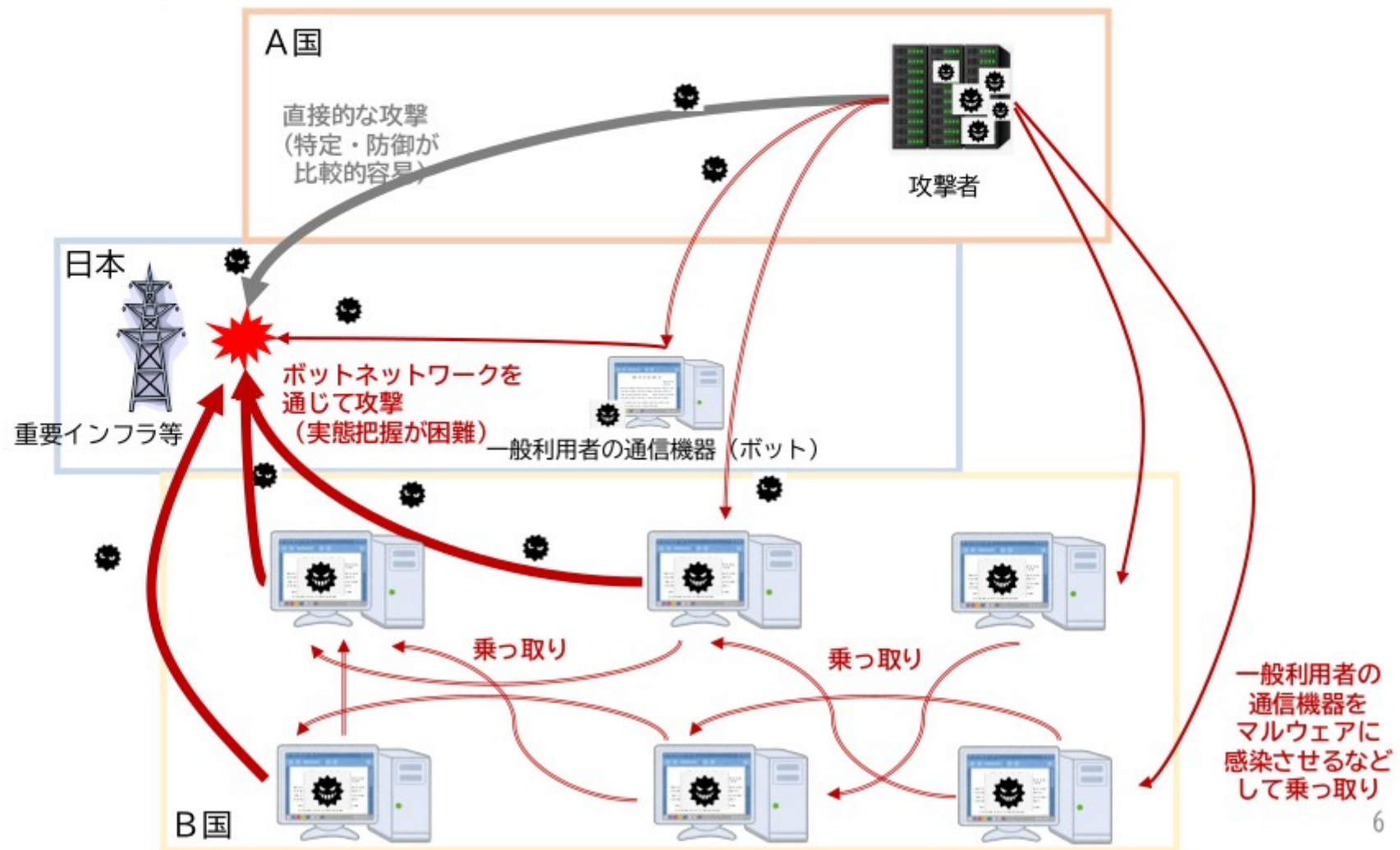
  これらには、従来型の諜報活動との連携が不可欠

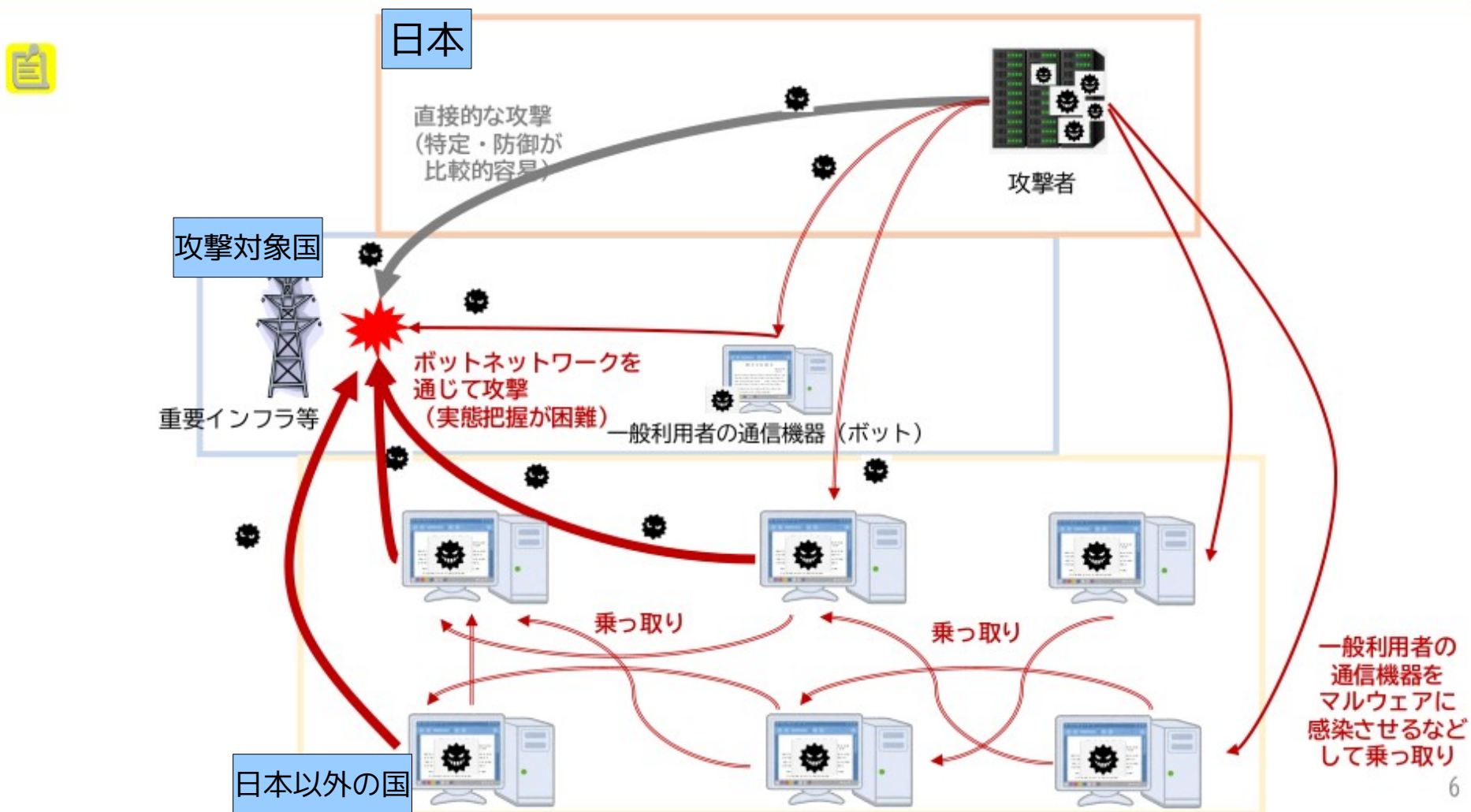
  米国などとの情報共有も不可欠
- Volt Typhoon は中国の攻撃である推測されているが、確証はない。

  サイバー攻撃では、攻撃の主体であることをカモフラージュすることが普通に行なわれる。

想定されるサイバー攻撃の経路の例（イメージ）

攻撃者は、攻撃元を隠蔽するため、一般利用者の通信機器をマルウェアに感染させるなどして乗っ取り、これらの通信機器（ボット）を多数、多段的に組み合わせて構成された攻撃用のネットワーク（ボットネットワーク）を利用することが通常。しかも、当該ボットの多くは、国外にも所在すると考えられている。このような状況で被害を防止するためには、ボットネットワークの実態把握が必要。

サイバー安全保障分野での対応能力の向上に向けた有識者会議 通信情報の利用に関するテーマ別会合 第１回事務局資料

能動的サイバー防御のイメージの一例

日本は、攻撃を隠蔽するため、一般利用者の通信機器をマルウェアに感染させるなどして乗っ取り、これらの通信機器（ボット）を多数、多段的に組み合わせて構成された攻撃用のネットワーク（ボットネットワーク）を利用する。しかも、当該ボットの多くは、他国にも所在させることで攻撃を隠蔽する。(サイバー安全保障分野での対応能力の向上に向けた有識者会議 通信情報の利用に関するテーマ別会合 第１回事務局資料を改変)

国家安全保障戦略

国家安全保障戦略（抄）

5

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、**サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる**。

【略】

武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。そのために、**サイバー安全保障分野における情報収集・分析能力を強化**するとともに、**能動的サイバー防御の実施のための体制を整備**することとし、以下の(ア)から(ウ)までを含む必要な措置の実現に向け検討を進める。

(ア) 重要インフラ分野を含め、**民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有**や、**政府から民間事業者等への対処調整、支援等の取組を強化**するなどの取組を進める。

(イ) **国内の通信事業者が役務提供する通信に係る情報を活用**し、**攻撃者による悪用が疑われるサーバ等を検知**するために、所要の取組を進める。

(ウ) **国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃**について、**可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与**されるようにする。

能動的サイバー防御を含むこれらの取組を実現・促進するために、**内閣官房サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組**し、**サイバー安全保障分野の一元的に総合調整する新たな組織を設置**する。そして、**これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備**、**運用の強化を図る**

国家安全保障戦略

このスライドの文言でいう能動的サイバー攻撃の前提条件は、

- 武力攻撃に至らない重大なサイバー攻撃のおそれ
- 安全保障上の懸念に該当し、かつ「重大」である

であるが、「至らない」「おそれ」「懸念」という現実には未だに何も攻撃や武力行使などが起きていない状況のなかで、将来そうした事態がありうると予測された場合、先手を打って攻撃に出る、ということになる。

議会や世論がこうした方針を支持するかどうかは、不安感情を政府がどれだけ煽ることに成功するかどうか、という情報戦にかかることになってしまうのではないか。こうした次のような懸念が生まれる。

- 現実の攻撃は存在しなくもよい。「懸念」「おそれ」があればサイバー攻撃を仕掛けるべきだ、という考え方は、先制攻撃そのものだ
- 導入される能動的サイバー防御の定義がないから、恣意的に運用できてしまう

国家安全保障戦略

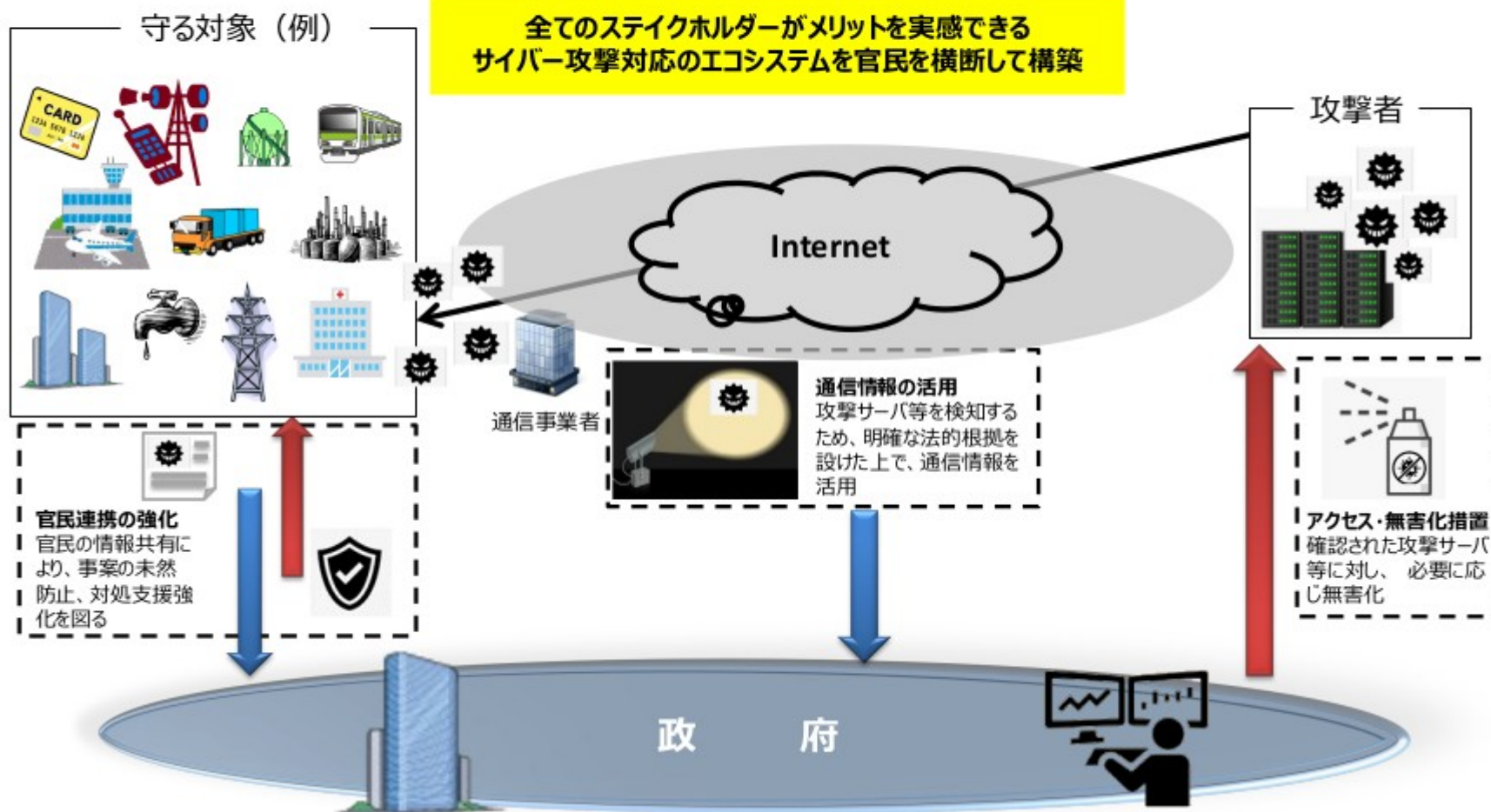
ここで能動的サイバー防御は、重要インフラを含めた民間事業者が、サイバー攻撃において様々な方法で積極的に関与する主体として位置付けられている。これは、サイバー領域全体の性格に共通する特徴でもある。民間インフラは、政府や自衛隊によって防衛される受け身の存在ではない。それ自体が国家安全保障を優先させ民衆の安全保障 2をそこなう「自衛」の主体とされ、それ自体が攻撃の主体にもなるのだ。民間の情報通信インフラ企業は、国家の命令による攻撃の主体になることによって防御を実現する、という位置に置かれる。言い換えれば、サイバー領域の軍事安全保障分野が他の軍事領域と決定的に異なるのは、民間事業者が情報収集から攻撃に至るプロセス全体の主体となることなしには成り立たない、という点にある。このスライドで例示されている Volt Typhoon の事例はその典型でもある。

国家安全保障戦略

このスライドで語られていない重要な問題

- サイバーと実空間(キネティック)における「攻撃」がサイバー領域の行動においてどのような関係をもっているのかが、全く語られていない
- その結果、能動的サイバー防御などサイバー領域での「戦争」が実空間での「戦争」と切り離されているかのような印象を与えている。
- サイバー領域での軍事作戦は実空間における武力行使と密接に関わる。サイバー領域で完結することはまずない。
- この認識は防衛省の制服組は明確にもっている。しかし、実空間との関連が問われることになると、該当する領域は極めて広範囲にわたり総力戦体制そのものとならざるをえず、当然憲法9条の制約問題が意識されるだろう。この問題化を回避する意図もあるのか、あえてサイバーと実空間とを横断する作戦の具体的な構造をあいまいにして、軍事安全保障の対処領域を意図的に狭くみせようとしている印象がある。

全体のイメージ

有識者会議第一回会議資料

全体のイメージ

ここには実空間における作戦との連携に言及がない。しかし防衛白書(2023 年)の次のような記述がある。

「万が一、抑止が破られ、わが国への侵攻が生起した場合には、わが国の領域に対する侵害を排除するため、宇 宙・サイバー・電磁波の領域及び陸・海・空の領域における能力を有機的に融合し、相乗効果によって全体の能 力を増幅させる領域横断作戦により、個別の領域が劣勢 である場合にもこれを克服しつつ、統合運用により機動的・持続的な活動を行い、迅速かつ粘り強く活動し続け て領域を確保し、相手方の侵攻意図を断念させる。」

アクセス・無害化
(Volt Typhoon)

外国におけるアクセス・無害化に関する取組例

【事例】米当局による取組

- 2023年５月、米国、カナダ、豪州、ニュージーランド及び英国は、中国の支援を受けたハッカーグループであるVolt Typhoonによるルータへの侵入や更なるハッキング、情報窃取への利用を合同で注意喚起。
- 米当局は、Volt Typhoonによる感染ルータがKV Botnet（ボットネット：マルウェアによるネットワーク）を構成していると特定。感染ルータに対し、**マルウェアの通信プロトコルを用いて、マルウェアを当該ルータから削除するコマンドを送信**するなど、必要な措置を実施。

（注）本事例のほか、

- **英当局**による**特定のAPT（高度な持続的な脅威）が用いる技術の弱体化**等の取組
- **カナダ当局**による政府ネットワークからの情報窃取防止を目的とした**サイバー犯罪者の海外サーバの無効化**等の取組

等が行われていることが公開資料等から明らかとなっている。

他方、こうした活動は**秘密の活動**として行われているものが多く、**以上についても詳細は明らかになっていない。**

有識者会議第一回会議資料

アクセス・無害化
(Volt Typhoon)

- 攻撃されたなかにはグアムのNTT子会社も含まれる
- FBIによるハッキング捜査

無害化のプロセスについて、
米国司法省は、 2024年1月31日にプレスリリースを発表し、同日テキサス州南部地区連邦検事局が連邦地方裁判所に捜索、差し押さえ令状発付の申請書を出す。

- リモートからルータ(大半はサポート期間が過ぎたCiscoおよびNetGearのルーター)を捜索
- マルウェアを削除
- 再度の感染を防ぐ措置をとる

Press Releases　Presskits　About

DOCOMO PACIFIC responds to multiple service outage

Tamuning, Guam (March 17, 2023) – DOCOMO PACIFIC, regional leader in innovation, telecommunications, & entertainment, works quickly to assess and restore service outage in Guam and the CNMI.

> *"Early this morning, a cyber security incident occurred and some of our servers were attacked. Immediate failsafe protocols were initiated by DOCOMO PACIFIC cyber security technicians to shut down affected servers and to isolate the intrusion. DOCOMO PACIFIC's customer data, mobile network services, and fiber services remain unaffected, protected, and secure at this time. We are working to restore service as soon as possible.*
> — Roderick Boss, President & CEO, DOCOMO PACIFIC

DOCOMO PACIFIC customers are encouraged to utilize their Mobile data to tether other devices such as laptops and tablets at no additional cost. Time of restoration is unknown.

Updates will be posted on DOCOMO PACIFIC'S social media. For more information or to discuss your service in detail, please call Guam 671-688-CARE or CNMI 670-488-CARE.

About DOCOMO PACIFIC

グアムのDOCOMO PACIFICの記者発表

アクセス・無害化
(Volt Typhoon)

Volt Typhoon とは誰なのか

欧米や日本のメディア報道や今回の内閣官房のスライドの記述では、中国の国策ハッカー集団であるという判断がほぼ確定している

中国側は、この指摘を受け入れてず、独自の報告書を公表。

- サイバー領域の「戦争」の難しさのひとつに、攻撃の責任主体を明確にすること (アトリビューション) 自体の困難さがある、と指摘。
- マイクロソフトや米国側が公表した資料を使い、 IP アドレスを分析するなかで、サイバー犯罪グループ Dark Power との関わりを指摘

中国の報告書の信憑性は？

- Dark Power であるという断定には証拠が不十分
- マイクロソフトのレポートも含めて、中国が Volt Typhoon の後ろ盾となっているということを立証した資料が米国側からも出されていないようだ

アクセス・無害化
(Volt Typhoon)

考えておくべき論点

- Volt Typhoon のアトリビューション問題は決着がついていない

  サイバー領域の安全保障にとって最重要の課題がアトリビューション問題。サイバー領域では、お互いに攻撃の主体であることを偽装しながら作戦を展開する極めてリスクの大きな領域であるにもかかわらず、米国が言うことだから間違いないといった対応はすべきではない。

- Volt Typhoon が無害化のひとつのモデルとして提示されているということであり、同じことを日本も実行できる法制度の条件が目論まれている
- Volt Typhoon では FBI の捜査対象が、国外ではなくグアムを含む米国内であった。つまり、国内であってもまた様々な手法による権力による私たちのコミュニケーション・インフラへの侵害行為がありうる。

アクセス・無害化
(Volt Typhoon)

考えておくべき論点 (続き)

- FBI がとったリモートからの侵入捜査と無害化の処理という手法には、今後の日本の捜査機関がサイバー安全保障の分野でとりうるであろういくつかの問題が示されている。
  - 多数の捜索対象に対して一つの令状で処理したこと。つまり令状主義が大きく後退していること。
  - リモートからの捜索とハッキングによる無害化という処理
- 今回は、捜査機関による何らかのソフトウェアのインストールなどより侵襲性の大きい行為のための令状は取得していない

  状況次第では、標的となったシステムへの何らかのソフトウェアなどのインストール (合法マルウェアなど) といった行動も令状さえ取得できればありうることを示唆

アクセス・無害化
(日本の事例)

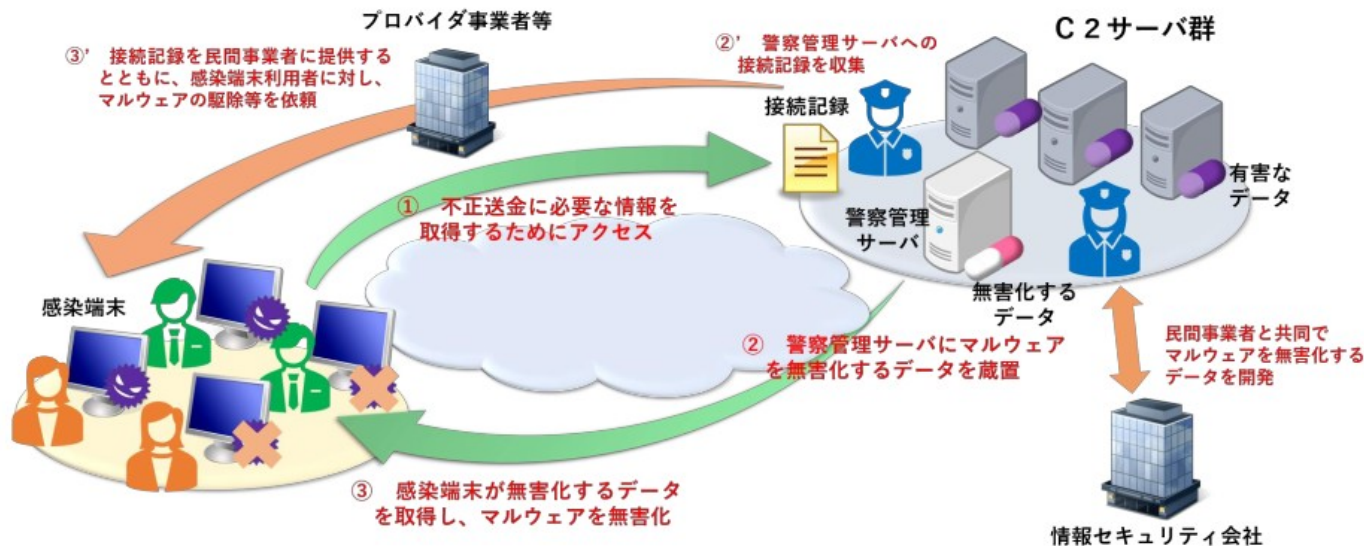
日本の前例 (第 2 回資料) 日本においても捜査機関による無害化の実行例がある。こうした行為が適法かどうか、また政府にはこれを自衛隊などが実行することへと拡大する意図があることを踏まえて批判の観点を明確に提起する必要がある。

アクセス・無害化措置に関連する警察の取組事例①

【感染端末内のマルウェアの無害化措置】

インターネットバンキングに係る不正送金事犯に係るマルウェアによる被害拡大の防止（平成27年）

- 平成27年４月、警視庁では、インターネットバンキングに係る不正送金事犯に使用されている**マルウェアの感染端末の通信先となっているC2サーバに割り当てられていた失効済みのドメインを取得し、警察管理サーバに割り当て**ることで、当該マルウェアの**感染端末情報の収集**を実施。
- 加えて、感染端末が指令を取りに行くためにC2サーバに定期的にアクセスすることを逆手に取り、**指令に関するデータの代わりに、マルウェアを無害化するデータを警察管理サーバに蔵置し、感染端末内のマルウェアの無害化措置を実施**。

有識者会議第二回会議資料

アクセス・無害化
(日本の事例)

アクセス・無害化措置に関連する警察の取組事例②

【任意の協力に基づくC2サーバの無害化措置】

不正アクセス事案における無害化措置（令和４年）

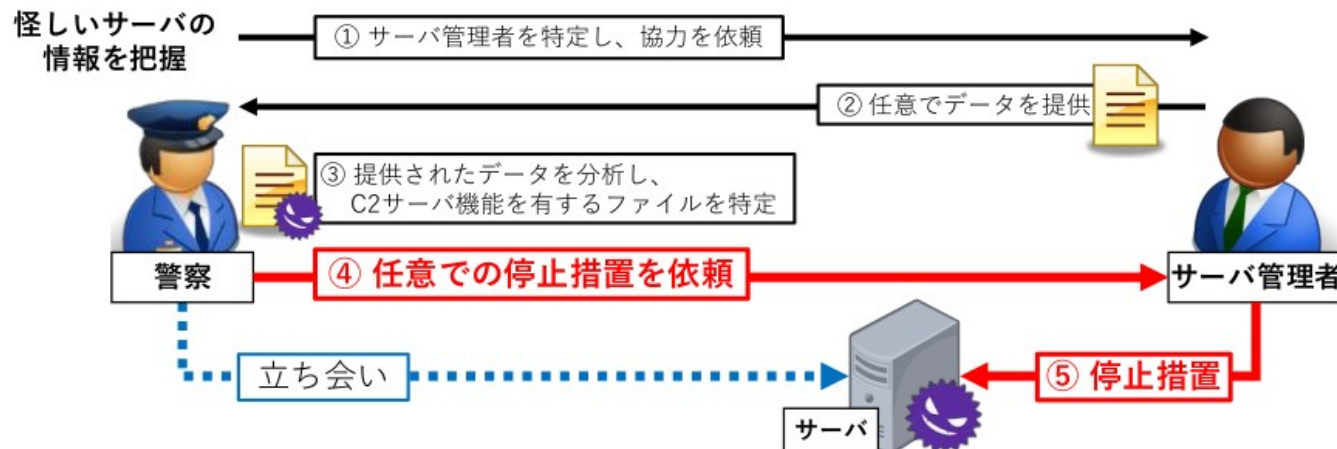
- 令和４年７月、警察において、あるwebサイトが改ざんされ、Ｃ２サーバとして利用されている疑いがある旨の情報を把握。
- **サーバ管理者（webサイト運営会社）を特定し、協力を依頼。**提供されたデータを精査し、**サーバ内の不審ファイルがＣ２サーバの機能を有することを特定。**
- **管理者の協力のもと、Ｃ２サーバの機能を停止**
  - ✓ サーバ内の不審ファイルの削除

不正指令電磁的記録供用事案における無害化措置（令和５年）

- 令和５年６月、警察において、マルウェアの通信先（C2サーバ）の疑いがあるサーバの情報を把握。
- **サーバ管理者（webサイト運営会社）を特定し、協力を依頼。**提供されたデータを精査し、**サーバ内の不審ファイルがC２サーバの機能を有することを特定。**
- **管理者の協力のもと、Ｃ２サーバの機能を停止。**
  - ✓ サーバ内の不審ファイル及び関連フォルダの削除
  - ✓ そのほか、使用していないwebサイトを閉鎖

「任意協力」という手法が積極的に用いられている模様だ。
任意協力として
- データの提供
- サーバーの停止措置

が挙げられている。

有識者会議第二回会議資料

アクセス・無害化
(日本の事例)

このスライドと次のスライドは無害化措置ができなかった事例である。無害化を実現するために国外の C2 サーバーへの攻撃が必要だということが含意されている。

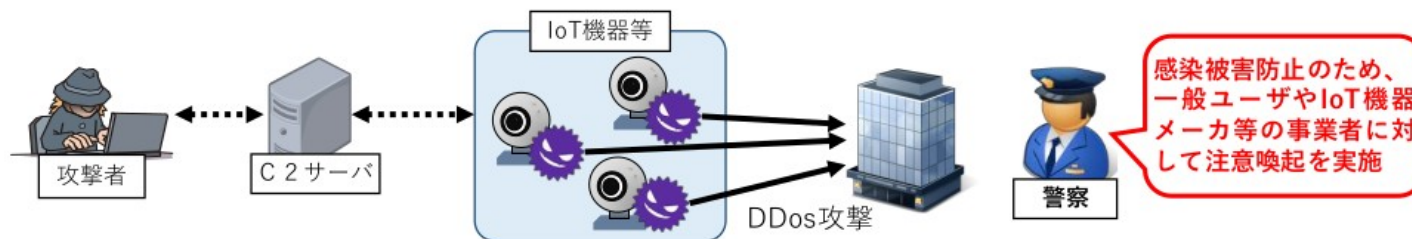
有識者会議第二回会議資料

アクセス・無害化
（日本の事例）

このスライドでは、たぶん「注意喚起」以上に立ち入った措置ができない、というところに無害化措置ができなかった原因を求めているように読める。これは、捜査機関などが私たちのパソコンにより容易に侵入して対処できる権限を求めているようにも読める。

無害化措置ができれば被害防止につながる可能性のある事例②

IoT機器等を踏み台としたサイバー攻撃を踏まえた注意喚起（平成28年～）

- 平成28年、国外において、IoT機器等に感染してDoS攻撃を行うマルウェア「Mirai」を使用したと見られるDDoS攻撃の被害が発生。
- 同年、警察庁のサイバーフォースセンターにおいて、**「Mirai」に感染したIoT機器等が発信元と見られる不審な通信の増加を観測。**
- **同年10月、警察庁では、ウェブサイトを通じて注意喚起を実施**するとともに、**一般財団法人日本サイバー犯罪対策センター（JC3）等と連携し、関係事業者に対する注意喚起を実施。**
  - ✓ ユーザ名、パスワードを推測されにくいものに変更。
  - ✓ 特定の接続先のみへのアクセス許可等、適切なアクセス制御の実施。
  - ✓ 最新のぜい弱性情報の確認とファームウェアの最新化等の適切な対策の実施。
- **平成28年以降も、**警察庁のサイバーフォースセンターにおいて、**「Mirai」の感染活動が観測されたことを踏まえ、ウェブサイトを通じた注意喚起を実施。**

⇒ IoT機器等の感染対策について再三周知しているものの、**現在でも、依然として「Mirai」に感染したIoT機器等が多数稼働している状況が確認**されている。

有識者会議第二回会議資料

現行制度の課題

現行制度上の課題

官民連携の強化　(ｱ)関係

- 高度な侵入・潜伏能力に対抗するため、政府の司令塔機能、情報収集・提供機能の強化が不可欠
  - ◆ 整理が必要な法令の例：サイバーセキュリティ基本法、各種業法

通信情報の活用　(ｲ)関係

- 悪用が疑われるサーバー等の検知には、「通信の秘密」を最大限に尊重しつつも、通信情報の活用が不可欠
  - ◆ 整理が必要な法令の例：憲法21条（通信の秘密）

アクセス・無害化措置　(ｳ)関係

- 重大なサイバー攻撃の未然防止・拡大防止を図るためには、政府に侵入・無害化の権限を付与することが不可欠
  - ◆ 整理が必要な法令の例：不正アクセス禁止法

- 上記の取組を実現・促進するため、強力な情報収集・分析・対処調整機能を有する新たな司令塔組織を設置することが必要。

有識者会議第一回会議資料

まとめ

大枠として有識者会議の資料で述べられていない重要な観点として、以下の点を挙げておきたい。

- 政府は憲法９条を一切考慮していおらず、サイバー領域における武力行使の問題がほとんど論点としても考慮されていないが、領域横断的な作戦のなかで用いられるという現実を念頭に置けば、９条問題は無視できないだけでなく、むしろ９条の枠組では戦争を阻止するには不十分ですらある。
- サイバー領域における自衛隊や日本の関連する省庁、企業の現状についての言及は一切ない。
- 米軍など同盟国側のサイバー領域での作戦についての現状についての言及はなく、一方的にロシア、中国などから攻撃されるケースのみが取り上げられている。